Fotograf: Mark Duffel

open systems

WORÜBER SPRECHEN CEOS UND VORSTÄNDE EIGENTLICH MIT IHREN CIOS?

Secure SD-WAN – damit CIOs ihre Ziele erreichen

Whitepaper

Vor Kurzem kam auf einem CIO-Event zum Thema hybride IT folgende Frage auf: «Worüber sprechen CEOs und Vorstände eigentlich mit ihren CIOs?».

Autor: Jack Miller, CISO von Open Systems

Der allgemeine Konsens lautete (in keiner bestimmten Reihenfolge):

1. Reduzierung der Kosten
2. Mehr Agilität und neue Technologien zur Unterstützung des digitalen Wandelstechnologies
3. Sicherheit und Compliance

Diese Liste war nicht wirklich überraschend. Es ist schwer vorstellbar, dass es eine IT-Abteilung gibt, die sich nicht mit diesen drei Themen beschäftigt. Doch bei genauerem Hinsehen scheinen sich die drei Aspekte zu widersprechen: Natürlich kann eine IT-Abteilung kleine Kosteneinsparungen erreichen, indem sie Druck auf Anbieter ausübt; doch wie sollen Ausgaben reduziert werden, wenn ständig neue Technologien zur Unterstützung des digitalen Wandels sowie für Sicherheits- und Compliance-Initiativen eingesetzt werden sollen? Die schnelle Implementierung neuer Technologien erhöht in

der Regel das Sicherheitsrisiko, und umgekehrt verlangsamt eine erhöhte Sicherheit den Einsatz neuer Technologien.

Sind die oben genannten Themenblöcke also realistisch? Können alle drei Ziele gleichzeitig erreicht werden? Die Antwort lautet glücklicherweise ja. Durch den Ausbau des vorhandenen WAN zu einem SD-WAN können Kosten eingespart werden. Gleichzeitig erhält man eine Infrastruktur, die den dynamischen Anforderungen des digitalen Wandels gerecht wird. Und mit der Implementierung eines Secure SD-WAN werden zugleich die allgemeine Sicherheit und die Compliance verbessert. So ist es nicht verwunderlich, dass laut einer aktuellen Studie 85 Prozent aller Unternehmen die Einführung eines SD-WAN in Betracht ziehen. Doch wie können mit einem SD-WAN diese Ziele erreicht werden und worin unterscheidet sich ein SD-WAN von einem Secure SD-WAN?

Kostenreduzierung

Die Anforderungen an die verfügbare Bandbreite haben sich in den vergangenen Jahren vervielfacht. Aus diesem Grund sind die Kosten für MPLS-Netze für Unternehmen mit vielen Standorten rasant angestiegen. Mittels SD-WAN können Unternehmen zusätzlich zu den MPLS-Netzen wesentlich günstigere Internetverbindungen nutzen, um ihren steigenden Bandbreitenbedarf zu decken. Auf diese Weise werden Grösse und Anzahl der benötigten MPLS-Netze reduziert und die Kosten erheblich gesenkt. So hat beispielsweise ein Kunde von Open Systems seine MPLS-bezogenen Kosten durch den Einsatz von SD-WAN um rund fünf Millionen US-Dollar pro Jahr reduziert. Solche Einsparungen sind ein Traum für jeden CIO.

Agilität und digitaler Wandel

Zwar können ältere WANs dynamische Routing-Protokolle wie OSPF oder RIP verwenden, doch sind sie zugleich relativ unflexibel. Derartige Routing-Protokolle haben den Vorteil, dass sie den Bedarf an manueller Konfiguration reduzieren und bei Netzwerkausfall oder Überlastung eine automatische Umleitung des Datenverkehrs in ein vermaschtes Netz ermöglichen. Dennoch bieten sie nicht die gleiche Flexibilität wie ein SD-WAN. Ein SD-WAN funktioniert anwendungsorientiert, und der Datenverkehr kann je nach Anwendung unterschiedlich gesteuert werden. So werden Traffic-Shaping und eine auf Anwendungskritikalität und Anforderungen basierende Priorisierung ermöglicht – das ist bei dynamischen Routing-Protokollen nicht möglich. Und da die Richtlinien zentral gemanagt werden und anwendungsbasiert sind, können neue Standorte oder Services zeitnah bereitgestellt werden. Cloud-Initiativen werden auf diese Weise erleichtert statt behindert.

Sicherheit und Compliance

Neben den oben genannten Vorteilen eines SD-WAN kann ein Secure SD-WAN dabei helfen, Sicherheits- und Compliance-Ziele zu erreichen. Was ist eigentlich der Unterschied zwischen einem SD-WAN und einem Secure SD-WAN? Richtig: die Sicherheit! Zwar verfügen SD-WANs über einige Sicherheitsfunktionen wie zum Beispiel Verschlüsselung – ein vollständig integriertes Sicherheits-Stack wie bei Secure SD-WANs fehlt jedoch. Doch ist das wirklich so wichtig? Absolut!

Ein Vorteil von SD-WAN ist die Unterstützung von Cloud-Initiativen mittels lokalem Internet Breakout, damit sich jeder Standort direkt mit dem Internet und der Cloud verbinden kann, ohne dass der gesamte Datenverkehr durch ein Hauptrechenzentrum geleitet werden muss. So kann ein lokaler Internet Breakout die Performance von Internet- und Cloud-Anwendungen erheblich steigern, führt jedoch zugleich zu neuen Herausforderungen in Sachen Sicherheit und Compliance. Denn an jedem Ort, an dem es einen Zugang zum Internet gibt, müssen die kompletten Sicherheitskontrollen implementiert werden. Statt nur einige Firewalls, Web-Proxys, IDS- und DLP-Systeme (um nur ein paar zu nennen) zu verwalten, ist dann möglicherweise das Management Hunderter solcher Sicherheitsvorkehrungen nötig. Jeder CISO wird Ihnen bestätigen, dass der extreme Mangel an qualifiziertem Security-Experten aktuell zu den grössten Herausforderungen gehört. Das Verwalten von zig mehr Systemen ist in diesem Kontext nahezu unmöglich, ganz abgesehen von den damit einhergehenden Ausgaben, die der gewünschten Kostenreduzierung entgegenwirken. Bei einem Secure SD-WAN sind all diese Kontrollen direkt in die SD-WAN-Lösung integriert, was sowohl die CapEx- als auch die OpEx-Kosten reduziert.

Die Replizierung des gesamten Internet Security Stack an jedem einzelnen Standort ermöglicht den Einsatz lokaler Internet Breakouts und mag so die Internet- und Cloud-Performance erhöhen – doch sorgt dies nicht für mehr Sicherheit oder Konformität als die Umleitung des gesamten Datenverkehrs durch ein zentrales Rechenzentrum. Ein Secure SD-WAN kann weit mehr. Das SD-WAN bietet umfassende Transparenz über den WAN-Datenverkehr. Die Kombination dieser Informationen mit den Logs des Security Stacks eines Secure SD-WAN erhöht die Erkennungsmöglichkeiten erheblich – und reduziert gleichzeitig die Auswirkungen und zeitlichen Verzögerungen, die mit möglichen Risiken verbunden sind. Doch die Erkennung ist nur der Anfang. Ein Secure SD-WAN ermöglicht darüber hinaus die automatische Segmentierung des Netzwerks, ohne dass der Betrieb unterbrochen werden muss. Kommt es zu einem Sicherheitsproblem an einer Stelle, werden dessen Auswirkungen damit so gering wie möglich gehalten. Ein Beispiel: Ransomware-Angriffe verbreiten sich oft über das WAN und infizieren auf diese Weise weit mehr Systeme, als wenn sie in dem LAN isoliert worden wären, in das sie ursprünglich eingedrungen sind. Die automatische Segmentierung des Secure SD-WAN isoliert den LAN-Datenverkehr, sobald es zum Ausbruch kommt. Das Schadprogramm erhält keinen Zugang zum WAN und somit nicht zu anderen LANs.

Doch wie alle anderen Technologien bringen auch Secure SD-WANs neue Herausforderungen mit sich. Dies gilt insbesondere für die Komplexität dieser Systeme, die Implementierungen oft erschweren. Aus diesem Grund entscheiden sich viele Unternehmen für ein Secure SD-WAN-as-a-Service. So sollten sich alle, die über die Implementierung eines Secure SD-WAN nachdenken, die Frage stellen, ob das eigene Personal die zusätzliche Komplexität und Arbeitslast bewältigen kann. Sollte das nicht der Fall sein, ist ein Secure SD-WAN-as-a-Service wahrscheinlich die optimale Lösung.

Über Open Systems AG
Seit 1990 ist Open Systems auf Netzwerke und Sicherheit für global tätige Unternehmen, NGOs und Institutionen fokussiert.
Das Unternehmen kombiniert Technologien, Prozesse und die beste menschliche Expertise, die auf dem Markt verfügbar ist.
Die ausgezeichnete Service- und Betriebsqualität wird mit einem der höchsten Kundenzufriedenheitswerte in der Industrie belohnt.

Open Systems AG, Räffelstrasse 29, 8045 Zürich, t +41 58 100 10 10, f +41 58 100 10 11, www.open.ch